

The complaint

A company which I'll refer to as O complains that Wise Payments Limited ('Wise') hasn't reimbursed the funds O lost as a result of a scam.

Mr S, who is a director of O, brings this complaint on O's behalf.

What happened

O's office manager was trying to pay a VAT bill to its accountant (I'll refer to this company as B in my decision). Initially the accountant sent O a link to a portal to make the payment but O's office manager experienced difficulties in paying via this method so B said O could pay the funds to its account. The accountant would then pay the bill via the portal.

On 8 June 2023 O's office manager made a payment to B via O's business account with Wise. Wise blocked the payment and asked that O's office manager confirm her identity. She contacted B to advise of the delay to the payment and received an email that appeared to come from B saying that the account was being audited and asking her to pay a different account. O's office manager didn't know at the time, but B's emails had been intercepted by a fraudster. B's genuine email address ended in '.co.uk' but the scam emails ended in '.com'.

O's office manager cancelled the original transaction and paid 37,985.89 AUD to the new account details provided (around £20,000). After the payment had been made, she received further emails that appeared to come from B and became concerned about the language used and the sense of urgency created. O noticed the slightly different email address on 21 June 2023 and contacted Wise to ask for the payment to be recalled.

O has commented that it doesn't appear Wise acted with any urgency when the scam was reported and that had it done so the outcome might have been different. Also, initially Wise told O's office manager that the payment would be returned because she hadn't spelled B's name correctly when the payment was made.

Wise didn't reimburse O's loss. It referred to the terms and conditions of O's account and said that it had contacted the bank that received the funds to try to recover them. There was a delay in Wise contacting the recipient bank so Wise checked whether its delay impacted the recovery of funds and established that funds were removed before the scam was reported.

Mr S, on behalf of O, was unhappy with Wise's response and brought a complaint to this service via a representative – the office manager who made the payment. Wise didn't provide its file, so the investigator issued his view on the information O provided.

Our investigation so far

The investigator who considered this complaint recommended that it be upheld in full. He said that the transaction was unusual, and Wise should have intervened. Given that there had previously been a problem with the payment, the investigator didn't think agents of O ought to have had concerns when the payment details were changed. He also noted that the intercepted email address was very similar to the real one.

Wise didn't agree with the investigator's findings. It provided evidence and said:

- O had made high value transactions prior to the scam payment so the payment aligned with the normal pattern of activity and there was no indication of a scam risk.

Wise provided examples, including a £61,200 transaction from O's GBP account on 18 July 2022 and multiple smaller value transactions between 1 and 9 March 2022 (including multiple payments to new payees).

- Whilst it acknowledged that there hadn't been any transactions on O's account for some time before the fraudulent transaction, it didn't agree an intervention was required. This was because O had a history of active account use in 2021 and 2022, transfer amounts varied from low value to over £61,000, consistent activity on the account led to a risk tolerance, and the transaction was in line with previous activity including an attempted previous payment to an account with the same name.
- Intervention levels for businesses are higher than for individuals.
- Although Wise maintains intervention was unnecessary it considered what would likely have happened if it had asked additional questions about the purpose of the payment and for evidence in support. Wise say that a representative of O would have explained that the payment was for VAT, was directed to O's solicitor (I think Wise means accountant), and could have provided appropriate documentation in respect of the requirement to pay VAT. Wise stressed that its due diligence process would not have involved questions regarding the accuracy of the recipient's details, or the possibility of the payment details being intercepted.
- Wise referred to its terms of use which say it isn't responsible for loss or damage that isn't foreseeable.

Mr S, on behalf of O, agreed with the investigator's recommendation but asked me to consider the following:

- If Wise hadn't asked for verification when a representative of O initially tried to make payment to B the scam wouldn't have taken place.
- O's representative assumed that Wise would check the payment was going to the correct company.

The complaint was passed to me to decide. I contacted Wise to ask for some additional information (about what happened when the initial payment to the legitimate company (B) was attempted) and to say that I thought it should refund O in full together with interest. Very briefly, this was because I thought the scam transaction was unusual and out of character so Wise should have intervened, at which point the scam would have been uncovered. This was because of its value, the fact the account had hardly been used in the 12 month period before the scam (except for a large transfer to an account linked to O and a small transaction), and the fact O was paying the same amount seemingly to the same payee but to different account details.

Wise provided the information requested and declined to reimburse O. I have summarised Wise's main points below:

- A representative of O attempted to make a payment to the genuine company B on 8 June 2023 and received a confirmation of payee match result. Wise asked for identification to complete the transfer, but this wasn't provided so the payment was automatically cancelled on 15 June 2023.
- O's representative uploaded her ID on 16 June 2023 and a few hours later made a new payment. The name of the company was the same as on 8 June (although misspelled), but the account details were different. The payment method (IBAN) wasn't supported by confirmation of payee. Wise said that uploading ID documentation and setting up a new transfer are normal and legitimate activities. And payee details changing is also not unusual as many firms of solicitors have multiple accounts.
- Turning to O's account history, Wise noted that before the £61,200 transfer from O's

account (to an account linked with O) on 18 July 2022 O received a similar amount from a third party account. Wise said that accepting high value payments like this poses a significant risk but as a responsible financial institution it conducted appropriate checks. As a result of these checks O's reliability was established and Wise had no reason to believe the transfer on 16 June 2023 wasn't to a legitimate recipient.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

In broad terms, the starting position in law is that an account provider is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the customer's account. And a customer will then be responsible for those transactions that they have authorised.

It's not in dispute here that O's office manager authorised the payment. So, while I recognise that she didn't intend the money to go to a scammer, the starting position in law is that Wise was obliged to follow O's instructions and process the payments. O isn't automatically entitled to a refund.

The regulatory landscape, along with good industry practice at the time, also set out an expectation for account providers to consider the interests of their customers and treat them fairly. And I think this included monitoring accounts to look out for unusual activity and trying to protect customers from fraud and financial harm. So I've also thought about whether Wise did enough to try to keep O's account safe.

After carefully considering O's account activity and the surrounding circumstances, I consider that Wise ought reasonably to have identified the scam payment as unusual and suspicious and taken additional steps before processing it. I will explain why.

I've considered O's account activity in the twelve month period before the scam. O had two accounts with Wise – a GBP account and an AUD account. The only transactions on the AUD account are a credit from a company linked to O on 6 June 2023, the attempted payment to the legitimate company on 8 June 2023 which was cancelled, and the scam transaction. Turning to O's GBP account, there was a credit of £61,680 on 15 July 2022 before a transfer was made to an account linked to O three days later for £61,200. Other than a £40 credit there were no further transactions until another small credit on 13 June 2023.

It's clear that O's accounts with Wise were rarely used at the time of the scam. The only large transaction from O's accounts was to a business account linked to O, which is very different to a transfer to a new third party account. Added to these points, a representative of O had recently attempted to make a payment to an account in the same name but with different account details. Taking into account the combination of these factors, I consider Wise ought reasonably to have recognised the risk of financial harm when the payment was made on 16 June 2023.

Wise has referred to the fact that the transfer to an account associated with O in July 2022 followed a credit from an external source of a similar amount. It says that the transactions established O's reliability and as a result it had no reason to believe O might be involved in fraudulent activity in June 2023. I'm not sure how these previous transactions could satisfy Wise that a transaction almost a year later to a totally different payee didn't carry any risk of fraud.

Wise has also referred to transactions from O's GBP account from August 2021 to 16 June 2022. Wise will be aware that when considering usual activity on an account this service generally considers account activity in the 12 month period before the scam. It's also clear that when these transfers were made there was regular activity on O's GBP account. This wasn't the case in the 12 month period before the scam transaction.

I'm satisfied that appropriate intervention by Wise would have uncovered the scam and prevented the loss. I see no reason why O's office manager wouldn't have told Wise the truth – that she had attempted to make a payment previously and had then been provided with new account details. Wise should have been alert to email intercept scams and the possibility that the payment details had been altered to divert funds to a scammer's account and provided appropriate warnings and advice. Such advice would include calling B to confirm the account details, at which point the scam would have been uncovered.

Wise said in response to the view that its due diligence process wouldn't have involved questions about the accuracy of the recipient details or covered email intercept scams so the scam would not have been uncovered. I'm satisfied Wise should have been alert to email intercept scams given their prevalence and that if it had only asked about the payment purpose it wouldn't have gone far enough.

I've also thought about whether O should bear any responsibility for its loss by way of contributory negligence. Like the investigator, I don't consider it should. O received fake emails that mirrored previous genuine emails and had no reason to believe anything was amiss.

As I think Wise should provide O with a full refund, I don't need to consider the efforts it made to recover O's funds. But briefly, I've seen evidence to confirm that funds were removed from the beneficiary account before the scam was reported to Wise so even if Wise had acted more promptly it wouldn't have made a difference.

Overall, I'm satisfied that Wise ought reasonably to have done more to protect O's account and should put things right by making the payments I have set out below.

My final decision

For the reasons stated, I require Wise Payments Limited to:

- Pay O 37,985.89 AUD
- Pay interest on the above amount at the rate of 8% simple per year from the date of loss to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask O to accept or reject my decision before 6 August 2024.

Jay Hadfield
Ombudsman